42 TEMAS PROCESALES

Vanessa Franco Ramírez
Editora

RED
Proceso y Justicia

2025-2 ISSN 2619-3655

Fundamentos teóricos y normativos de las pruebas digitales[1]

Geraldo Prado[2]
Universidad Autónoma de Lisboa
consultoria@geraldoprado.com
https://orcid.org/0000-0002-4738-780X

> En la práctica del juicio procesal, la estructura peculiar del dato digital engendra la ilusión de que lo que está digitalmente representado es indiscutible, así como el sentido atribuible a esa representación. Ello nos lleva a creer de manera acrítica que una exhibición digital es adecuada para apoyar el razonamiento lógico-probatorio del juez[3] (Brighi & Ferrazzano, 2021, p.14).

Resumen

El artículo esboza los fundamentos del tratamiento jurídico de las precauciones orientadas a mantener la integridad, la autenticidad y la auditabilidad de las pruebas digitales obtenidas mediante el acceso directo o remoto a sistemas informáticos. Los fundamentos teóricos y normativos de las pruebas digitales, esto es, sus presupuestos, no vienen determinados tan solo por el poder de injerencia en

---

1 Conferencia «Fundamentos teóricos y normativos de las pruebas digitales», pronunciada en Medellín (Colombia), el 11 de octubre de 2025, en el panel «Proceso, prueba e interdisciplinariedad: nuevas fuentes de la prueba», en el ámbito del «Foro Internacional Tutela Judicial Efectiva y Prueba: un desafío contemporáneo», promovido por la Institución Universitaria de Envigado (IUE), la Universidad de Cádiz (UCA) y la Red para el Estudio del Proceso y la Justicia (RED). En esa ocasión, se presentaron los resultados parciales de la investigación llevada a cabo sobre el fenómeno de la transnacionalidad del proceso penal, tema que se aborda en el contexto del Proyecto de I+D Corpus Delicti – Estudos de Criminalidade Organizada Transnacional [Ratio Legis - Centro de Investigação e Desenvolvimento em Ciências Jurídicas, de la Universidad Autónoma de Lisboa - UAL].

2 Doctor en Derecho. Investigador de Ratio Legis - Centro de Investigação e Desenvolvimento em Ciências Jurídicas, de la Universidad Autónoma de Lisboa, y profesor visitante de la Universidad Autónoma de Lisboa. Miembro del Comité de Asesoramiento del Instituto de Direito Penal e Ciências Criminais, de la Facultad de Derecho de la Universidad de Lisboa. Miembro del Consejo Científico del Centro de Investigação em Justiça e Governação, de la Universidad de Minho (JusGov). Consultor Senior Asociado del JusticiaLatinoAmerica – JusLat (Chile). Integra el Núcleo de Investigación Defensiva de la Defensoría Pública del Estado de Río de Janeiro (NIDEF). Consultor Jurídico. Exprofesor Asociado de Derecho Procesal Penal de la Universidad Federal de Río de Janeiro (UFRJ). Consultor Jurídico. Currículo Lattes disponible en: http://lattes.cnpq.br/0340918656718376.

3 Traducción libre del original. En adelante todas las traducciones del español al italiano son por cuenta del autor.

la vida privada y de tratamiento automatizado de los datos. El fenómeno probatorio actual es muy diferente del escenario que predominó durante siglos hasta hace poco más de diez años. Hoy en día, los profesionales del Derecho se enfrentan a pruebas generadas de manera automática mediante sistemas de inteligencia artificial, que no tienen relación con una determinada realidad empírica. La opacidad de los sistemas informáticos que procesan la información digital y constituyen las pruebas digitales es antagónica a la publicidad procesal. Las pruebas digitales no están sujetas al mismo estatuto epistemológico que las pruebas tradicionales, requieren un tratamiento jurídico-procesal compatible con su condición de objeto digital y el potencial engañoso de su forma final —su resultado— es insuficiente para asegurar su admisibilidad en el proceso, dada la volatilidad y la posibilidad de manipulación de los datos, imperceptible si no se comprueba técnicamente su autenticidad, integridad e integralidad. El peritaje oficial es una etapa relevante en la formación de la prueba digital. La manipulabilidad de esta prueba no permite que, en el ámbito jurídico, la formen sujetos que tienen intereses o que actúan de acuerdo con hipótesis fácticas preestablecidas.

Palabras clave: investigación digital, investigación intrusiva, acceso a dispositivos digitales, control judicial, cadena de custodia.

Theoretical and regulatory foundations of digital tests

Abstract

The article outlines the foundations of the legal treatment of precautions aimed at preserving the integrity, authenticity, and auditability of digital evidence obtained through direct or remote access to computer systems. The theoretical and normative foundations of digital evidence—namely, its underlying premises—are not determined solely by the power of interference with private life and the automated processing of data. The current evidentiary landscape differs markedly from the scenario that prevailed for centuries until little more than a decade ago. Today, legal professionals face evidence generated automatically by artificial intelligence systems that bear no direct relationship to a specific empirical reality. The opacity of the computer systems that process digital information and constitute digital evidence is antagonistic to procedural publicity. Digital evidence is not subject to the same epistemological status as traditional evidence; it requires a procedural legal treatment compatible with its condition as a digital object, and the potentially misleading nature of its final form—its result—is insufficient to ensure its admissibility in court, given the volatility and the possibility of data manipulation, which is imperceptible unless its authenticity, integrity, and completeness are technically verified. Official forensic expertise is a relevant stage in the formation of

digital evidence. The manipulability of this type of evidence does not allow, within the legal sphere, its formation by individuals who have vested interests or who act in accordance with pre-established factual hypotheses.

Keywords: digital investigation, intrusive investigation, access to digital devices, judicial control. chain of custody.

1. Consideraciones en forma de esbozo

En 1971, Mario Losano publicó, en la *Revista Trimestral de Derecho Público*, de Italia, un artículo titulado «Por un Derecho compatible con la elaboración electrónica» (Losano, 2022), en el que reconsideraba y, en cierta medida, ampliaba el planteamiento que había llevado a cabo, en 1969, en su *Iuscibernética: máquinas y modelos cibernéticos en el derecho* (Losano, 2022), adelantando décadas los debates por los que solo recientemente los juristas han mostrado un mayor interés. En ambos textos, por ejemplo, Losano aborda la tensión entre el principio de eficiencia y otros valores que, en la administración de la justicia, deben prevalecer sobre aquel.

A principios de 2025, Orin Kerr, profesor de la Escuela de Derecho de Berkley, presenta su tesis sobre la *4.ª Enmienda Digital*, en la que, por otros derroteros, sostiene la idea de un nuevo constitucionalismo digital norteamericano que se configura, de manera inevitable, teniendo en vista el carácter disruptivo de las tecnologías digitales modernas (Kerr, 2025).

Es un constitucionalismo caracterizado por una serie de decisiones de los tribunales norteamericanos, entre ellos el Tribunal Supremo, en las que se definen los límites al ejercicio del poder en la esfera digital. Como afirma Kerr (2025), «nuestros derechos no deben quedar a merced de los cambios tecnológicos» (p.4)[4] y cita, como ejemplo, la sentencia de 2014 del caso *Riley c. California*,[5] en la que se exige que exista un requerimiento judicial y una orden para efectuar un registro en un aparato de telefonía móvil.

La preocupación que ronda a ambos, a Losano y Kerr, con más de cincuenta años de diferencia entre los textos citados, deriva del reconocimiento de las características disruptivas de las tecnologías digitales contemporáneas y su impacto en la configuración de la realidad, no solo por el carácter intrusivo que es característico de estas aplicaciones tecnológicas, sino también porque la *realidad* que *constituyen* no se apoya necesariamente en elementos empíricos, cosas

4 Traducción del inglés al español hecha por el autor.

5 Tribunal Supremo De Los Estados Unidos. Concepto del Tribunal pronunciado por el magistrado John Glover Roberts Jr., en Riley c. California, 573 U.S. (2014). n. 13-132, el 25 de junio de 2014. Juzgado junto con United States c. Wurie, n.º 13-212.

tangibles o hechos del mundo de la vida que un conjunto seguro de informaciones pueda *representar* retrospectivamente, esto es, mediante *prueba jurídica*.

Para ilustrar el argumento basta comprender que el resultado de aplicar la inteligencia artificial (IA), para tratar, de manera simultánea y a una velocidad imperceptible para los sentidos humanos, datos de geolocalización, gastos efectuados mediante tarjetas bancarias, publicaciones en redes sociales y movimientos financieros puede definir el *perfil digital* de una persona y este no es un dato de la realidad, sino el *producto* de un análisis, es decir, la *interpretación* de un conjunto extraordinario de informaciones en matriz digital, procesadas en los términos de la lógica computacional.

Con el fin de comprender lo que es la implementación de la IA de manera simultánea y a una velocidad imperceptible para los sentidos humanos, conviene saber que el superordenador Frontier tiene una capacidad de procesamiento de hasta 1.1 trillones de operaciones de puntos fluctuantes por segundo (Figueiredo, 2024).

En este sentido, el nuevo escenario de la época actual, que Comoglio (2018) denonima «Petabyte age» (p.234), se asimila mejor si se recuerda, con Kerr (2025), que la transformación tecnológica disruptiva anterior, que tuvo lugar en la década de 1920, derivó de la popularización del automóvil, un medio de transporte que, en cierto modo, anonimizaba al conductor y le permitía, por ejemplo, cargar rápidamente mercancías cuya tenencia era ilícita y huir de la policía.

Fueron estas características del automóvil, desconocidas cuando se publicó la 4.ª Enmienda a la Constitución norteamericana (People of the United States, 1791), las que, en 1925, hicieron que el Tribunal Supremo modificara su criterio sobre la exigencia de una orden judicial para el registro de vehículos, al declarar constitucional la nueva regla derivada del criterio policial en este tipo de situaciones, sin orden, siempre que hubiera una *causa probable* (*Carroll c. Estados Unidos*) (Kerr, 2025).

Kerr (2025) afirma que los automóviles transformaron la vigilancia policial en el siglo XX y el «Tribunal respondió con un aluvión de nuevas reglas jurídicas solo para los coches» (p.2).

A diferencia de lo que pasó en los años veinte del siglo pasado, la nueva *revolución tecnológica*, por su extraordinario potencial intrusivo en la intimidad, bastante bien conocido, y su capacidad de procesar a gran velocidad una cantidad impensable de datos personales, expandió de forma drástica el poder de los gobernantes y las grandes corporaciones tecnológicas, como constata el profesor de Berkley (Kerr, 2025).

Los fundamentos teóricos y normativos de las pruebas digitales, esto es, sus presupuestos, no vienen determinados tan solo por ese dramático poder de injerencia en la vida privada y de tratamiento automatizado de los datos.

Aún en 2008, al tratar de lo que, en aquella época, se denominó *prueba electrónica*, Michele Taruffo (2014) alertaba de los peligros «de falsificación, errores y uso indebido o abusos [que] son especialmente frecuentes y relevantes y, en cierta medida, [son] aún desconocidos» (p. 84). La conclusión de Taruffo, en aquel momento, acerca de la admisibilidad de este tipo de prueba, no podía ser diferente: «En suma, decir que el valor probatorio de las pruebas informáticas se deja a la valoración discrecional del juzgador puede parecer una forma de eludirse del problema y no solucionarlo» (p.87).

La afirmación de Taruffo se remonta al tiempo en el que, en comparación con nuestros días, las aplicaciones de inteligencia artificial no afectaban tan de lleno a la prueba digital o electrónica y en el que, aunque erróneamente se trataba de forma análoga a la prueba tradicional (testigos, objetos dotados de existencia material, documentos en papel, etc.), parecía posible equipararlas.

El fenómeno probatorio actual es muy diferente del escenario que predominó durante siglos hasta hace poco más de diez años. Hoy en día, los profesionales del Derecho se enfrentan a pruebas generadas de manera automática mediante sistemas de inteligencia artificial, que no tienen relación con una determinada realidad empírica, como sucedía con el cadáver de una persona, un arma, etcétera (Camargo, 2025).

Al abordar la *Admisibilidad de la prueba a la luz de la revolución digital*, la profesora italiana Quattrocolo (2023) analiza los fundamentos teóricos y normativos de las pruebas digitales, teniendo en cuenta el que constituye el aspecto central de la materia desde el punto de vista de la función probatoria de los elementos digitales: su capacidad demostrativa. Las pruebas sirven para *demostrar* un determinado hecho.

Mientras que las pruebas que, a efectos de la presente comunicación, se denominan acá *pruebas tradicionales* están ancladas en una precisa realidad empírica, que les permite *representar* un hecho —un homicidio, un robo, una violación, etc.—, la prueba digital no *representa otra realidad* que no sea la propia combinación algorítmica, que no es más que una determinada «serie de operaciones técnicas cargadas de variables que transforman [los datos] en diferentes resultados posibles, de voz, imagen, texto, etc., conforme se procesen esas secuencias de *bits*» (Brighi y Ferrazzano, 2021, p. 14).

Como lo recuerdan Brighi y Ferrazzano (2021), el *dato digital* consiste en una representación de secuencias de *bits* incomprensibles para los humanos, que requieren interpretación: «[Los] datos [por sí solos] no pueden tener ningún significado» (p.14).

Si esto es verdad en relación con las fotografías, los audios o los mensajes de texto digitales —es decir, esas fotografías, audios y mensajes de texto no *existen* en el mundo real solo con la forma como los percibimos tras resultar del proceso

técnico de su conversión—, los jueces y demás profesionales jurídicos se depararán cada día, cada vez con más frecuencia, con *objetos digitales* cuyo *input* ya no será humano, a diferencia del *fotografiar*, *grabar* o *escribir un mensaje de WhatsApp* que sí lo es (Yuk, 2023).

Dispositivos digitales remotos de vigilancia continua (por ejemplo: drones, infiltración digital, dispositivos de videovigilancia, ubicación o reconocimiento facial-GPS, etc.) e informes elaborados de forma automática gracias al tratamiento de una cantidad casi infinita de información disponible en el mundo digital y de mecanismos digitales de búsqueda automatizada mediante la selección de información extraída de fuentes abiertas pueden funcionar con independencia del *input* humano. Son aplicaciones de IA programadas para *aprender automáticamente* (*machine learning*), sin intervención humana.

Es cierto que el potencial *demostrativo* de las pruebas tradicionales, su capacidad de *representación de la realidad*, siempre ha estado condicionado por la interpretación que hacen los sujetos procesales. La confrontación entre declaraciones contrapuestas, la interpretación del informe pericial acerca de la falsedad de un documento, de la relación de imputación entre la acción y la lesión o el estudio de si, en el producto examinado, se encuentra o no una determinada droga son situaciones susceptibles de interpretación. No obstante, la diferencia con la prueba digital, que cambia por completo el escenario actual, es que el juez y las partes no están en condiciones, por sí solas, de *interpretar* la prueba digital, determinar su autenticidad, integridad, integralidad o, incluso, comprenderla y explicarla como el *objeto digital* que es.

En este sentido los mundos probatorios se separan. El mundo probatorio digital, de la prueba digital cuyo *input* haya sido humano o de la generada totalmente de manera automatizada, no es autoexplicable o autoevidente. Esos elementos probatorios ni siquiera encajan en la clasificación, a la que nos hemos acostumbrado, de *pruebas preconstituidas* y *pruebas procesales* (que denominamos *constituendas*) (Quattrocolo, 2023, p.175) y no se someten a la que las clasifica en fuentes personales y fuentes reales. Las fuentes de las pruebas digitales son *digitales*, esa es su matriz.

Las pruebas digitales, formalmente, son preconstituidas. Su proceso de preconstitución, no obstante, difiere de las pruebas preconstituidas tradicionales porque la propia prueba digital se caracteriza como un *proceso*. La *prueba digital* no existe en su *resultado*, o solamente en su resultado (la fotografía, el audio o el vídeo digital).

Su condición *lógica* depende de una sucesión de etapas técnicas que se inician con su *recopilación* y que pasan por varias fases destinadas a su verificación, interpretación, explicación, rastreabilidad y supervisión humana.

Es destacable un ejemplo de Richard Feynman, premio nobel de física, que en 1985, al responder a la pregunta de «si las máquinas pueden pensar como humanos

y ser más inteligentes que ellos», afirmó que las máquinas no pensarían como los humanos, al igual que los aviones no vuelan como los pájaros (ICHI.PRO, s.f.). La prueba digital *no vuela como los pájaros*, no tiene las características de las *pruebas tradicionales*, que deben acoplarse a la realidad empírica.

No es pertinente adentrarse ahora en el debate acerca del dominio de los *softwares* (los derechos de propiedad inmaterial sobre dichos *softwares*) que participan en todo el proceso de constitución de la prueba digital y que caracterizan la *externalización* de la persecución penal, pero es necesario acotar que hay consenso acerca de que las constituciones de los Estados democráticos someten la validez jurídica de las decisiones judiciales a la publicidad de los actos procesales. Se prohíbe el secreto, de modo que la hipotética reserva o sigilo sobre determinados actos no es oponible a los representantes de las partes. La *opacidad* de los sistemas informáticos que *procesan* la información digital y constituyen las pruebas digitales es antagónica a la publicidad procesal. En este caso, el concepto jurídico de *publicidad* también debe adaptarse a la *realidad digital*.

Aunque no se aborde el extenso debate entablado entre la doctrina del derecho digital acerca del significado de *transparencia*, lo cierto es que, en contra de la *opacidad* de los sistemas digitales, en particular de aquellos de generación automatizada, se impone la *transparencia*, cuya naturaleza es doble: lógica y jurídica.

Por un lado, siguiendo a Quattrocolo (2023), se trata de una especie de *transparencia por persona interpuesta*, en la medida en que deben precisarse las etapas técnicas del proceso de formación de la prueba (lo que se conoce como *explicabilidad* de la prueba digital de modo amplio).

El Tribunal de Casación italiano, en una decisión de 7 de septiembre de 2022, en el famoso caso EncroChat, se posicionó en contra de la legalidad del *hackeamiento* masivo, cuando no se informe a la defensa, durante el proceso, del método para llevarlo a cabo, y subrayó expresamente que «el principio de contradicción implica que la dialéctica procesal no se aplique solo al material obtenido, sino que se amplíe a la forma de obtención de dicho material» (Zaragoza Tejada, 2024, p. 312).

Eliminar la *opacidad digital* exige que la persona que participa en todos los procesos de formación de la prueba digital domine, como especialista, conocimientos multidisciplinares muy específicos. La publicidad, respecto a la prueba digital, es *publicidad digital*, por lo que no se puede conformar con la prueba como *resultado*.

Por otro lado, la prueba de matriz digital, *que el especialista incauta técnicamente* y *verifica*, debe *traducirse* por partida doble: en sus propios términos técnicos, con los aparatos adecuados, y en lenguaje natural, para los interesados, las partes y el juez o jueza.

Si el proceso de formación de la prueba digital no es *comprensible*, y no solo su resultado, no se puede efectuar ningún juicio de valor sobre elementos cognoscitivos de matriz digital. La explicabilidad es fundamental y el especialista, que se constituye como *sujeto procesal principal*, funciona como *conector*, como señala Kaufman (2022), profesora de la PUC de São Paulo.

Kaufman (2022) afirma que el hecho de que los algoritmos establezcan correlaciones en los datos que no son perceptibles para los desarrolladores humanos es el origen del problema de la interpretabilidad o *black box* (p.17). La profesora de la PUC de São Paulo se refiere a los «habitantes de las tierras fronterizas» (p.19), que serían los especialistas, como ejemplo de *conectores* entre los desarrolladores de los sistemas de inteligencia artificial y los destinatarios de sus aplicaciones.

Creo que es inevitable que los especialistas informáticos, con una formación multidisciplinar, sean esos *habitantes de las tierras fronterizas*, que explicarán a los interesados, las partes y el juez o jueza, en un lenguaje accesible, las diversas etapas de formación de la prueba digital, indicando los métodos y los recursos aplicados, su adecuación a la prueba digital concreta, así como su interpretación técnica sobre la autenticidad, la integridad y la integralidad de la referida prueba (De Menezes, 2014).

A este respecto, Quattrocolo (2023) aclara que «la *transparencia* certifica el proceso computacional; la *explicabilidad* permite la accesibilidad, en lenguaje no computacional, al recorrido que llevó del *input* al *output*, aumentando los espacios de evaluación de las específicas finalidades que se consideren» (p.174).

La explicabilidad, que abordará todas las etapas de formación de la prueba digital, funciona como una regla de exclusión probatoria para cuando se constaten violaciones técnicas que comprometan la autenticidad, la integridad, la integralidad y la auditabilidad de la prueba digital.

La auditabilidad de esa prueba —que toma la forma de rastreabilidad de su proceso— configura la contradicción digital, como señaló el Tribunal italiano. Su afectación, así como la de la autenticidad y la integridad de la prueba, hace imposible saber si el *objeto digital* que se trata como prueba fue alterado de forma intencionada o accidental y, de modo que se comprometió su *representación digital de* algo. Se trata de una causa de inadmisibilidad de la prueba por la imposibilidad de verificarla.

En un voluminoso estudio sobre los protocolos de conservación de la prueba digital, Di Iorio (2018) afirma que las precauciones específicas que se exigen en el ámbito internacional para este tipo de prueba tienen en cuenta el propósito de «evitar la contaminación de la prueba», en general, resultante de una actividad indebida de identificación, adquisición y conservación de la prueba digital, con lo que se logra «minimizar la manipulación de la prueba digital», «documentar cualquier acción que implique un cambio irreversible» en la mencionada prueba,

separar rígidamente la función pericial de cualesquiera otras asociadas a la investigación digital («no extralimitarse de sus competencias y no tomar decisiones sin la autorización correspondiente») y, valga señalar, «adherirse a las regulaciones y leyes locales» (Di Iorio, 2018, pp.341-343).

Son bastante interesantes a este respecto los artículos 7 y 8 de la Propuesta de Directiva del Parlamento Europeo y el Consejo de Europa acerca de los criterios y parámetros para la admisibilidad de la prueba digital en los procesos penales (European Law Institute, 2023).

Además, es sabida la característica de la volatilidad de los datos. Al tratar de la prueba digital en el proceso judicial, Meireles (2025) afirma, con razón, que

> [la] posibilidad de que se adulteren las pruebas digitales, dada su fragilidad, lleva a que, no solo en el nivel informático, sino en lo que a nosotros nos respecta, en el campo jurídico, sea la consigna para exigir más a este tipo de prueba, porque nunca podremos equipararla a una simple prueba documental.

Pero no solo eso. Existen dos aspectos que, en general, pasan desapercibidos en las investigaciones criminales y los procesos penales, pese a su carácter fundamental: el acceso masivo o significativo a datos de terceros, con ocasión de la incautación de elementos probatorios digitales; y las acciones prospectivas infiltradas o con carácter de hipervigilancia digital, que se producen en el *entorno digital* del propio sospechoso, sin su conocimiento.

En el primer caso, la potencial amplitud casi ilimitada de la acción cautelar invasiva —del *registro digital*— preocupó, por ejemplo, al Tribunal Constitucional Federal alemán, así como a buena parte de la doctrina que se ocupa del tema de la prueba digital (Barros et al., 2025; Bundesverfassungsgericht, 2024).

Cuando se lleva a cabo una operación policial en la que se produce la incautación de dispositivos electrónicos o se accede a canales o plataformas digitales (en las *nubes*), los datos obtenidos no se refieren solo a los sospechosos, los investigados o, incluso, las víctimas. La mayoría de los casos, se obtienen datos de numerosas personas que no guardan ninguna relación con las investigaciones.

Un régimen constitucional que valore la autodeterminación informativa debe tener en cuenta que existe la posibilidad de manipular esos datos y la necesidad de protegerlos contra su uso indebido.

En un artículo reciente, el comisario de la Policía Federal brasileña Stenio Santos Sousa advierte acerca de la cuestión: «¿Cómo tener la firme convicción de que ese vestigio digital presentado en juicio se obtuvo, recabó o produjo exactamente de la forma descrita en la investigación criminal?» (Sousa, 2025, p.635).

Sousa (2025) alerta, en particular, sobre las actuaciones de investigación que se efectúan directamente en un *entorno digital*, como es el caso de la *infiltración*

digital de agentes, que permite, e incluso potencia, que el agente infiltrado digital altere ese entorno. El referido autor añade la indagación que sirve de guía a todos los reglamentos contemporáneos sobre la cadena de custodia de la prueba: «¿Cómo garantizar que el agente público, tras acceder a un dispositivo informático, no aprovechó la oportunidad para alterar el entorno cibernético, incluyendo información u otros datos que confirmen la hipótesis de investigación?» (Sousa, 2025, p.635).

Por consiguiente, la preocupación con la autenticidad, la integridad y la integralidad de los elementos de prueba de matriz digital tiene en cuenta una serie de factores, además de aspectos relacionados con la correcta manipulación de esos elementos, para protegerlos frente a accidentes, selecciones sesgadas o parciales y alteraciones intencionadas o no que, en el plano de los fundamentos teóricos y normativos de las pruebas digitales, acentúan la ya referida importancia de los *especialistas*, esos «habitantes de las tierras fronterizas».

En el ámbito del derecho procesal penal, ¿quiénes son esos *especialistas*, habitantes de las tierras fronterizas, y qué deben hacer? Para responder a estas preguntas, siempre hay que tener presente que la *e-evidence*, prueba electrónica o prueba digital se caracteriza por ser «cualquier clase de información (datos) que haya sido producida, almacenada o transmitida por medios electrónicos» (Delgado Martín, 2022, p.55).

La definición de *prueba digital* del Instituto Nacional de Tecnologías de Comunicación de España (Inteco) se plantea en estos términos y destaca el binomio software-hardware que es peculiar a ciertos elementos probatorios digitales. Esta definición recalca el *proceso de recogida por medio de herramientas técnicas especializadas empleadas por un perito en investigación informática* como parte integrante de la noción de prueba digital (Bueno de Mata, 2019, p.133).

El *especialista* o perito en investigación informática es el sujeto procesal que, adoptando técnicas establecidas en protocolos nacionales e internacionales, actúa en el proceso de *constitución de esa prueba* buscando asegurar, desde la obtención al resultado, el uso escrupuloso de los parámetros relativos a cada tipo de prueba digital.

Ramalho (2017), autor de un laborioso estudio sobre la fase de la *obtención* de la prueba digital, examina los principales modelos teóricos de *recolección* de esa prueba, de los que presenta sus respectivas ventajas y desventajas. Un aspecto común a los diversos modelos consiste, en la intervención del experto informático, pues todos los métodos «exigen rigor científico en la recogida de la prueba» (p.114).

En el libro *La cadena de custodia de la prueba en el proceso penal* (Prado, 2022) se describen ampliamente los cuidados que exigen algunas importantes normativas internacionales que, en sus respectivos ámbitos, regulan el *acceso* a

las pruebas digitales. En común con la posición que defiende Ramalho (2017) se encuentra el hecho de que el procedimiento debe dirigirlo un *especialista forense*.

Ese especialista siempre es necesario, aunque un ejemplo de su imprescindibilidad puede verse en la necesidad de «intervenir en los sistemas informáticos afectados directamente en el lugar donde estos se encuentren» (Ramalho, 2017, p.119), lo cual es en especial importante cuando los referidos sistemas «estén conectados y en funcionamiento [pues] habrá que salvaguardar de inmediato los datos más volátiles, a fin de evitar que sea imposible su recuperación» (p.119).

En Portugal, Ramalho (2017) diferencia, en el plano doctrinal, la intervención del especialista forense de la del perito, «en el sentido jurídico procesal del término» (p.133), porque, aunque a ambos los nombre la autoridad judicial, el perito estaría encargado de efectuar un *examen* del material incautado, algo que a su juicio, escaparía de la actividad de *recogida* de la prueba digital, su «detección, incautación y conservación» (p.137). Sin embargo, sobre este aspecto, Ramalho cae en el error que él mismo denuncia cuando critica con dureza la equivocada equiparación de las pruebas tradicionales y las digitales.

En relación con las pruebas tradicionales, el examen de los vestigios que hace el perito busca determinar algún aspecto del hecho a probar, como el nexo de causalidad entre la hipotética acción que se atribuye al sospechoso y el resultado de dicha acción, que se materializa en una alteración del mundo exterior. ¿Fueron los disparos de arma de fuego que alcanzaron a la víctima la causa eficiente de su muerte? Normalmente, los *peritos oficiales* se ocupan de este tipo de exámenes, que exigen una conclusión sobre la existencia de un determinado hecho.

El *perito digital*, ese especialista informático que exigen todas las normativas conocidas en materia de prueba digital, desempeña otra función, para la que, empero, se necesita tener conocimientos específicos de naturaleza multidisciplinar, en general en el campo de las ciencias de la informática, que usa en diversos momentos, desde la obtención de los dispositivos e información digitales y la extracción de los datos al análisis de las condiciones de su conservación y su puesta a disposición a las partes mediante copias forenses.

No es por el hecho de que el perito, en esta función, no se pronuncie sobre *nexos de causalidad* o *contextos de imputación* que se desvirtúa su función y pertinencia. Por el contrario, si se considera la necesaria imparcialidad que debe orientar la actuación de los implicados, que asegura a los interesados, las partes y el juez o jueza la autenticidad, integridad e integralidad de los datos, el binomio fundamental de esta forma de peritaje está presente: *neutralidad*, frente al contexto de la investigación, y *dominio técnico*, para garantizar la adecuada *constitución* de la prueba digital.

En el contexto de enorme vulnerabilidad de la prueba digital, en ningún caso su formación puede ser responsabilidad de los interesados o las partes, aunque

se trate de la víctima o del Ministerio Público. En Brasil, la sección 5.ª del Superior Tribunal de Justiça (2023) dictó una decisión paradigmática al respecto.

La actuación del peritaje oficial en todo proceso de formación de la prueba digital deriva, en Brasil, del sistema del Código de Proceso Penal (CPP), que reserva a las partes (o, en la investigación, a los interesados) la constitución de un asesor técnico. Como sugerencia y teniendo en cuenta la realidad, máxime en un país con el tamaño continental de Brasil y los significativos índices de criminalidad, que carece de servicios periciales en la mayoría de los municipios, parece conveniente establecer que, en la actuación de incautación de dispositivos digitales (computadoras portátiles o de mesa, *tablets*, relojes inteligentes, teléfonos celulares o móviles, etc.), ante la fundada imposibilidad de que los peritos oficiales puedan estar presentes en las actuaciones, se sigan rigurosos protocolos para la obtención de esos dispositivos, bajo la supervisión a distancia del perito, y se elabore un minucioso informe sobre las condiciones de la actuación.

En el caso de que se obtengan datos directamente de los canales (*nubes de datos*), son los proveedores quienes deben proporcionar los enlaces a los peritos y nunca otro sujeto procesal, con lo que se evita el problema antes mencionado. También este proceso está sujeto a incidentes que pueden perjudicar la formación de la prueba.

En ambos supuestos, el Ministerio Público, la Policía y las defensas y los eventuales representantes de las víctimas deben tener acceso únicamente a las copias forenses, de modo que el objeto digital se mantenga en poder del servicio pericial. También parece fundamental que toda transferencia de datos solo pueda realizarse bajo supervisión presencial o remota de un perito, en la que se especifiquen el método utilizado y las condiciones antes referidas, a ser posible con el registro audiovisual íntegro del acto.

El documento de incautación de dispositivos digitales ha de ser mucho más completo que las denominadas actas de incautación de bienes, pues debe indicar quién es el sujeto encargado de intervenir en el entorno digital, su condición de especialista, la situación en la que encontró los objetos digitales y las razones que justifican la elección de los métodos utilizados para la obtención de la prueba.

Lo que a primera vista impresiona por su complejidad es, en realidad, algo bastante rutinario en el ámbito de la práctica de los *especialistas informáticos*, forma parte de su día a día y quienes siguen, por ejemplo, las recientes actuaciones de los peritos criminales federales ya deben haberse topado con estos informes.

Por último, la *cadena de custodia* de la prueba digital no se confunde con su documentación. Su objetivo es asegurar *la formación de la prueba digital* para permitir su uso en el contexto jurídico, proporcionando condiciones para afirmar su autenticidad y completitud y asegurando la explicabilidad de su proceso y su rastreabilidad (auditabilidad) a fin de facilitar la contradicción digital.

Lo que se pretende al establecer y mantener la cadena de custodia de la prueba digital, en primer lugar, es garantizar el acceso adecuado a información digital y su conservación para usarla en un contexto jurídico. La documentación de la cadena de custodia, de acuerdo con lo establecido en los artículos 158-A a F del CPP,(Presidência da República, Decreto-Lei Nº 3.689, 1941) debe retratar el proceso de su instauración y conservación.

2. Conclusiones

En resumen, las pruebas digitales no están sujetas al mismo estatuto epistemológico que las pruebas tradicionales; requieren un tratamiento jurídico-procesal compatible con su condición de objeto digital, y el potencial engañoso de su forma final —su resultado— es insuficiente para asegurar su admisibilidad en el proceso, dada la volatilidad y la posibilidad de manipulación de los datos, imperceptible si no se comprueba técnicamente su autenticidad, integridad e integralidad.

El peritaje oficial es una etapa relevante en la formación de la prueba digital. La manipulabilidad de esta prueba no permite que, en el ámbito jurídico, la formen sujetos que tienen intereses o que actúan de acuerdo con hipótesis fácticas preestablecidas, como es el caso de la Policía, el Ministerio Público, las víctimas, los sospechosos o los acusados.

Referencias

Barros, F. de M., Marinho, L. A., & Sarkis, J. M. (2025). A etapa do descarte na cadeia de custódia dos vestígios digitais. En C. Badaró Massena, & A. P. Melchior (orgs.), *Estudos Jurídicos em homenagem ao professor Geraldo Prado por seu 65º aniversário* (pp. 223-250). Marcial Pons.

Brighi, R., & Ferrazzano, M. (2021). Digital forensics: best practices and perspective. En M. Caianiello, & A. Camon (eds.), *Digital forensic evidence: towards common European standards in antifraud administrative and criminal investigations* (p. 12-48). CEDAM.

Bueno de Mata, F. (2019). *Las Diligencias de Investigación Penal en la Cuarta Revolución Industrial: principios teóricos y problemas prácticos*. Aranzadi.

Bundesverfassungsgericht. (2024, 1 de octubre). *Headnotes to the Judgment of the First Senate of 1 October 2024 1 BvR 1160/19*. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2024/10/rs20241001_1bvr116019en.html

Camargo, P. L. de A. (2025). *Inteligência artificial na investigação criminal: parâmetros de transparência e explicabilidade*. Thomson Reuters.

Comoglio, P. (2018). *Nuove tecnologie e disponibilità della prova. L'accertamento del fatto nella diffusione delle conoscenze*. Giappichelli.

Delgado Martín, J. (2020). *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia: Obtención, tratamiento y protección de datos en la justicia*. Wolters Kluwer.

Di Iorio, A. (2018). Protocolos de preservación de evidencia digital y cuestiones forenses. En D. Dupuy (dir.), M. Kiefer (coord.), *Cibercrimen II*. (pp. 341-343). Editorial B de F.

De Menezes, P. B. (2014). *Novos rumos da prova pericial*. 7Letras.

European Law Institute. (2023). *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute*. European Union – Universitat Wien. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf

Figueiredo, A. L. (2024, 2 de diciembre). Supercomputador Frontier recria o universo em simulação inédita. *Olhar Digital*. https://olhardigital.com.br/2024/12/02/ciencia-e-espaco/supercomputador-frontier-recria-o-universo-em-simulacao-inedita/

ICHI.PRO. (s.f.). Richard Feynman sobre Inteligência Artificial Geral. *ICHI.PRO*. https://ichi.pro/pt/richard-feynman-sobre-inteligencia-artificial-geral-4849711885060 9#google_vignette

Kaufman, D. (2022). *Desmistificando a inteligência artificial*. Autêntica.

Kerr, O. (2025). *The Digital Fourth Amendment: Privacy and Policing in Our Online World*. Oxford University Press.

Losano, M. (2002). Per un diritto compatibile con l'elaborazione elettronica. En P. Garbarino, & M. Cavino (eds.), *Scritti di informatica e diritto: per una storia dell'informatica giuridica. Vol. 2* (pp.393-414). Mimesis Edizione.

Meireles, A. I. D. (2025). *A Prova Digital no Processo Judicial: a blockchain e outros caminhos para os tribunais*. Almedina.

People of the United States. (1791). *Constitution of the United States: Fourth Amendment*. Senate of the United States. https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm#amdt_4_1791

Prado, G. (2022). *La cadena de custodia de la prueba en el proceso penal* (2ª. ed.). Marcial Pons.

Presidência da República. (1941, 3 de octubre). *Decreto-Lei Nº 3.689 de 1941* [*Código de Processo Penal*]. https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm#art810

Quattrocolo, S. (2023). L'ammissione della prova alla luce della rivoluzione digitale. En E. M. Catalano, & P. Ferrua, Paolo (eds.), *Corderiana. Sulle orme di un maestro del rito penale* (p. 163-176). Giappichelli

Ramalho, D. da S. (2017). *Métodos Ocultos de Investigação Criminal em Ambiente Digital*. Almedina.

Sousa, S. S. (2025). A cadeia de custódia como garantia de fiabilidade dos elementos de interesse em formato digital. En C. Badaró Massena, & A. P. Melchior (orgs.). *Estudos Jurídicos em homenagem ao professor Geraldo Prado por seu 65º aniversário* (pp. 621-642). Marcial Pons.

Superior Tribunal de Justiça. (2023, 14 de febrero). *Informativo n.º 763 del Tribunal Superior de Justicia, de 14 de febrero de 2023*. Agravo Regimental en el Habeas Corpus n.º 143.169/RJ. Quinta Turma do Superior Tribunal de Justiça [M. P.: Messod Azulay Neto, M. A] [Ponente de la sentencia: Dantas, R.].

Taruffo, M. (2014). *A prova* (J. G. Couto, trad.). Marcial Pons.

Yuk, H. (2023). *Sobre la existencia de los objetos digitales* (A. Cordero y D. Wiehls, trads.). Materia Oscura.

Zaragoza Tejada, J. I. (2024). La prueba ilícita y prueba tecnológica. Reflexiones a raíz del caso Encrochat. En J. C. Ortiz Pradillo, & A. Abellán Albertos (dir.), *El derecho de defensa en la justicia penal digital* (pp. 241-348). Tirant lo Blanch.

42 | TEMAS PROCESALES
2025-2
Foro Internacional
Tutela Judicial Efectiva y Prueba
2025

RED
Proceso y Justicia

La presente edición de Temas Procesales reúne un conjunto de investigaciones que reflejan la diversidad, complejidad y actualidad del debate procesal contemporáneo. Con aportes provenientes de España, Colombia, Brasil e Italia, esta revista ofrece al lector un recorrido por problemáticas emergentes y enfoques renovados que dialogan entre la teoría, la práctica judicial y los desafíos tecnológicos que atraviesan el derecho en la actualidad.

Abrimos con un análisis sobre trastornos del lenguaje y pruebas personales, una reflexión necesaria para comprender cómo las condiciones comunicativas inciden en la credibilidad, la percepción judicial y las garantías procesales. A continuación, un estudio sobre los fundamentos teóricos y normativos de las pruebas digitales aborda su creciente centralidad en los sistemas de justicia y los retos que plantean para la autenticidad, integridad y cadena de custodia.

Italia aporta un texto sobre la valoración de las pruebas y su control por la Corte di Cassazione, que permite observar cómo este tribunal ha construido criterios de racionalidad y límites para el juez de mérito. En materia tecnológica, el artículo sobre prueba científica y tecnologías de registro distribuido profundiza en la fiabilidad, trazabilidad y potencial probatorio de sistemas como blockchain. Se suma un estudio sobre lingüística forense y su utilidad para la identificación y atribución de mensajes, seguido de un análisis del criminal compliance program y la prueba en el proceso penal español, especialmente relevante para organizaciones sujetas a responsabilidad penal.

La edición continúa con una reflexión sobre la prueba en la determinación de la filiación, así como un aporte teórico sobre injusticia algoritmico-epistémica y valoración probatoria, tema crucial ante el avance de sistemas automatizados de decisión.

Finalmente, dos estudios inspirados en Taruffo cierran este número: la cientifización del proceso en lo contencioso administrativo colombiano y el principio de precaución ambiental como argumento en la creación judicial del derecho. Esta revista invita a pensar, comparar y transformar nuestras prácticas procesales desde una perspectiva plural y rigurosa.

ISSN 2619-3655